

will be seen from the discussion that follows, the architecture described in the reference does not anticipate this invention, as amended. In this invention, both signature and verification occur on a single server, without distribution of public keys to message recipients, which is completely different from the discussion and diagrams of the cited authors. While the office action of March 12, 2001 cited Message Authentication Codes (MACs) as one reason why the symmetric encryption signature of this invention was anticipated by prior art, the authors specifically excluded at p. 320 the use of MACs as a signature protocol suitable for purposes of non-repudiation, because both the recipient and originator shared the key, and either could have affixed the encryption. In this invention, a symmetric key is used by a single server for signature and verification functions. Thus, one of the novel aspects of the invention is the ability for the first time to use MACs as signatures by virtue of the single server having sole possession of the symmetric key, which is a new, non-obvious and patentable characteristic novel over prior art.

The procedural context of this application is thus somewhat unusual, in that the final action was taken upon a brand new prior art reference of the Applicant never discussed or referenced in any prior submissions, rejections or the responses of the Applicant, and a totally new basis of rejection has been adopted. Given this sweeping and dramatic change, Applicant was unable to amend the claims before and respectfully requests the continued patience of the examiner in order to resolve what appears to be an overly broad interpretation of the prior art reference, which is the primary basis for the office action rejection, dated March 12, 2001.

Specification

The examiner objected to new matter consisting of an illustrative example of a marked up page on page 7 at the bottom, as follows: "In a normal transaction, assuming a template consists of text *a, b, c* and more text *e, f, g* and still more text *i, j, k*; with spaces that a user fills in with transaction specific information *d* and *h*; then by way of illustrative example, the digital wrapper which is assembled for the signature at the server consists of *abc + d + efg + h + ijk + GUID*." The illustrative example has been deleted and leave has been requested to replace it instead with the simple textual phrase: "The digital wrapper includes the GUID and text supplied by a user which is assembled with the template at the server for signature."

Former claim 35 (now claim 55)

The examiner objected to former claim 35 because it was in improper form. The claim cited two other claims and thus suffered from multiple dependencies. The claim which has been renumbered as new claim 55 has been amended to remove one of the independent claim references, which was unnecessary and confusing in any event. The applicant thanks the examiner for pointing out this defect, which has been corrected. Request is therefore made to consider now this claim on the merits.

Section 112 Objections and Rejections**A. General**

The examiner rejected the claims on the basis of Section 112, stating that the claims failed to point out and distinctly claim the subject matter of the invention. Claimant has requested leave to amend the former independent claim 20, now renumbered as claim 40 by striking the ultimate clause in the claim and substituting the following in its place:

whereby the document is both electronically signed on behalf of a client user and verified by a relying party using the server computer, without any client-side encryption keys distributed to any signing or relying party, or a need for interoperability of keys, certification authorities, or other methods of identifying users to individual keys in their possession.

In light of this change, applicant respectfully requests the examiner to reconsider the rejection of this and the other affected claims, which have also been similarly amended.

B. Specific

The examiner noted in paragraph 9 of the OA that former claim 20 incorrectly stated in the final clause that a client user signed the document. The new claim 40 now corrects the defect by stating instead that the document is signed on behalf of the client user.

The examiner stated in paragraph 10 of the OA that various portions of former claim 20 contained indefinite clauses without recitation of intended limitations, as well as former claim 23 and former 30. The defects have been corrected in new claims renumbered as claims 43 and 50. The defect in former claim 35 has been corrected by removing the offending reference, as is noted earlier in this requested amendment.

The examiner stated in paragraph 12 of the OA that the phrase "or other methods" rendered the claim indefinite. Leave is sought to remove the phrase by amendment.

The Rejections on the Basis of Ford, et al. under Section 102 Are Overcome

The O.A. dated March 12, 2001 rejected claims 20, 21, 24, 26 and 27 (now redrafted claims 40, 41, 44, 46 and 47) pursuant to section 102 (b) as being anticipated by Ford et al. "Secure Electronic Commerce." Applicant respectfully requests reconsideration of this rejection, as now applicable to the redrafted claims, for the following reasons.

As the Court stated in *Jamesbury Corp. v. Litton Industrial Products Inc.*, 756 F.2d 1556 (Fed. Cir. 03/12/1985),

Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim. *Soundscriber Corp. v. U.S.*, 175 Ct. Cl. 644, 360 F.2d 954, 960, 148 U.S.P.Q. (BNA) 298, 301, 149 U.S.P.Q. (BNA) 640 (1966).

The standard is not met on the basis of Ford et al. Ford et al describe elements not present in the instant invention: These include: 1. optional signing by the originator of the document prior to submission for signature to the trusted third party, 2. verification of the trusted third party's signature at the recipient's location using the public key of the trusted third party in the possession of the recipient , 3. authentication of the source and data integrity of the message from the originator prior to signing, and 4. non-optional return of the document to originator for transmittal to the recipient. See Ford et al page 332 and Figure 8.2 by way of example. Items 1-3 are all absent from this invention. Item 4 is not mandatory in this invention. The elimination of

items 1-3 and the differences in item 4 establish the physical novelty of the invention over Ford et al.

There are also elements in this invention which are missing from Ford et al and which independently establish the physical novelty of the present invention. This invention allows for many methods of authentication of persons and entities on whose behalf signing occurs, while Ford et al limit examples of permissible authentication to two methods which the authors deem secure, being public key authentication and Kerberos. These latter two methods have been excluded from redrafted claim 49 which now expressly provides for their exclusion in language that is identical to that contained in endnote 35 of Ford et al which describes the examples given by Ford et al. Only the methods which are excluded by Ford et al are included in the redrafted claim.

In redrafted claim 41 and the claims dependent upon it, a unique identifier is generated for each and every document that is signed on behalf of a user, which is absent from the description in Ford et al. Claim 41 does include a time and date factor as part of the unique identifier, but this is mandatory in claim 41 and is only optional in Ford et al. Also, claim 44 concerns the use of voice commands to effectuate user actions. Claim 47 concerns electronic agents. These are totally absent from Ford and therefore are not properly a basis for a §102 rejection.

Redrafted claim 46 provides for an optional client side digital signature **after** the server's digital signature is applied, while Ford et al describe an originator's signature being affixed **prior to** the application of the signature by the trusted third party, which is an important reverse sequencing of signatures establishing a difference in the claim and the prior art. Again, these differences establish the physical novelty of the invention over Ford et al.

Accordingly, the applicant respectfully submits that the claims of this invention are not anticipated by Ford et al., and are patentable over Ford et al. (Secure Electronic Commerce) notwithstanding section 102(b).

Section 103 Rejections

There are a number of section 103 rejections. What follows is a discussion of the law that is applicable to section 103 rejections generally and is therefore useful with regard to each of the specific rejections.

The Court of Appeals for the Federal Circuit in *Northern Telecom Inc. v. Datapoint Corp.*, 908 F.2d 931 (Fed. Cir. 06/29/1990) ¶¶ 32-34 has stated:

It is insufficient that the prior art disclosed the components of the patented device, either separately or used in other combinations; there must be some teaching, suggestion, or incentive to make the combination made by the inventor. *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143, 227 USPQ 543, 551 (Fed. Cir. 1985) (insufficient to select from the prior art the separate components of the inventor's combination, using the blueprint supplied by the inventor); *Rosemount, Inc. v. Beckman Instruments, Inc.*, 727 F.2d 1540, 1546, 221 USPQ 1, 7 (Fed. Cir. 1984) ("As this court has held, 'a combination may be patentable whether it be composed of elements all new, partly new or all old'" (citations omitted); *W. L. Gore & Assocs., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1551, 220 USPQ 303, 312 (Fed. Cir. 1983), cert. denied, 469 U.S. 851, 105 S. Ct. 172, 83 L. Ed. 2d 107 (1984) (individual references can not be "employed as a mosaic to recreate a facsimile of the claimed invention.")
....

As discussed in *In re Rothermel*, 47 C.C.P.A. 866, 276 F.2d 393, 397, 125 USPQ 328, 332 (CCPA 1960), the nature of the problem "which persisted in the art", and the inventor's solution, are factors to be considered in determining whether the invention would have been obvious to a person of ordinary skill in that art. See also, e.g., *Fromson v. Advance Offset Plate, Inc.*, 755 F.2d 1549, 1556, 225 USPQ 26, 31 (Fed. Cir. 1985) (the prior art must suggest to one of ordinary skill in the art the desirability of the claimed combination).

See also *In re Zurko*, 142 F.3d 1447, 1459, 46 USPQ2d 1691, 1701 (Fed. Cir.) (en banc), cert. granted, 119 S. Ct. 1816 (1999)(on other grounds):

[T]he Board impermissibly used hindsight to arrive at the claimed invention. See W.L. Gore & Assocs., Inc. v. Garlock, Inc., 721 F.2d 1540, 1553, 220 USPQ 303, 312-13 (Fed. Cir. 1983) ("To imbue one of ordinary skill in the art with knowledge of the invention in suit, when no prior art reference or references of record convey or suggest that knowledge, is to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher.

With regard to rejections based upon matters outside the record, such as taking official notice, the guidelines entitled FORMULATING AND COMMUNICATING REJECTIONS UNDER 35 U.S.C. 103 FOR APPLICATIONS DIRECTED TO COMPUTER-IMPLEMENTED BUSINESS METHOD INVENTIONS adopted pursuant to the Supreme Court case of *Graham v. John Deere* (1966), available online at <http://www.uspto.gov/web/menu/busmethp/busmeth103rej.htm>, state:

Prior art includes all public knowledge demonstrating the level of ordinary skill in the art. The examiner may take official notice of facts outside of the record which are capable of instant and unquestionable demonstration as being "well known in the art." While an examiner may reject a claim based on common/prior knowledge in the art, this practice is to be applied sparingly. It is always incumbent upon the examiner to find a reference to support a rejection. If the applicant traverses such an assertion the examiner should cite a reference in support of his or her position. When a rejection is based on facts within the personal knowledge of the examiner, the data should be stated as specifically as possible, and the facts must be supported, when called for by the applicant, by an affidavit from the examiner. Such an affidavit is subject to contradiction or explanation by the affidavits of the applicant and other persons. See 37 CFR 1.104(d)(2).

With these principles in mind, a request is made to reconsider the various Section 103 rejections, each of which is discussed below.

The Rejection of Claims 22 and 29 on the basis of Ford et al (Secure Electronic Commerce) are overcome.

The O.A. rejected former dependent claims 22 and 29, now claims 42 and 49 on the basis of Ford et al. These redrafted claims include authentication by means of a shared secret or biometric device from the client computer to the server computer. Ford et al. expressly limit permissible authentications to other methods which in their opinion assure data integrity and message authentication of the source, and do not allow for shared secrets by means of passwords or PINS, or biometrics across a network. Ford et al expressly limit their examples of permissible network authentications to public key or Kerberos authentications. Such authentications have been excluded from the redrafted claim 49 by the exclusion as follows: "but excluding authentication based on local domain security services on a client-server network with public-key or Kerberos authentication and key establishment." This language is virtually identical to that contained in endnote 35 of Ford et al, which can be found in the amended supplemental Form 1449 and attached pages from the work which is filed herewith.

The Rejection of Claims 23 and 28 on the basis of Ford et al (Secure Electronic Commerce) are overcome.

The examiner rejected claim 23, now redrafted claim 43, on the basis of Ford et al in paragraph 17 of the O.A. dated March 12, 2001. The examiner acknowledged that although Ford et al did not say an archive of signature transaction is undertaken, official notice could be taken that data archiving was an old practice. The reasoning, with all due respect, conflicts with the diagram furnished by Ford et al and the language of the work. No database of signature identifications is created or maintained at the trusted third party in Ford et al because in a Public Key Infrastructure (PKI), which the authors support and this invention does not, there is no storage of such characteristics ever undertaken at the trusted third party. Only the certificates of users that link them to keys and lists of revoked certificates are stored in a database at the trusted third party. Information about specific signature transactions is not. That is a major new and unusual result of the signature technology of this invention.

In this invention, the relevant characteristics of each signature transaction is stored, rather than certificate information that links the identities of users to client-side keys as in a PKI. Ford et al show signature information storage occurring at the *recipient's* computer in the diagram Figure 8.2, not at the server. That is the reverse of this invention. In this invention, the server, which is

analogous to the trusted third party of Ford et al, stores the information about each signature in a database, never the recipient. Ford et al do not suggest this invention. The practice of archiving data does not itself suggest this invention. Ford et al are at odds with the architecture of this invention. Section 103 does not apply. The invention is novel in light of Ford et al.

The applicant respectfully traverses the assertion of official notice and requests a reference or affidavit of the examiner.

The examiner also rejected claim 28, now redrafted claim 48, on the basis of Ford et al in paragraph 17 of the O.A. dated March 12, 2001. While acknowledging that Ford et al. do not mention Message Authentication Codes, official notice was made that MACs can be used to create to provide something that works as a signature.

With all due respect, Ford et al teach exactly the opposite from the official notice that is asserted. They expressly state on p. 320 as follows. (See the amended 1449 with attached pages, filed herewith):

“Recall that a MAC is a symmetric cryptographic mechanism – both the originator and recipient of a message share a common key. The originator uses the key to generate the MAC and the recipient uses the same key to verify the MAC. This mechanism can provide authentication and data integrity – the recipient can be confident of who originated the message and that the message was not modified, provided it is known that only the two parties possessed the key. However, a MAC cannot provide non-repudiation of the origin of a message because it is not adequate *to convince a third party* as to who originated the message – since two parties possessed the key, either one could equally well have originated the message.” (Emphasis original)

Under the circumstances, Applicant respectfully requests the examiner to reconsider the invocation of official notice. In this invention, only one party, which is the server, ever possesses the symmetric key, both for signing and verifying a signature. Since only one party (the server) and never two parties possesses the symmetric key, the system does not suffer from the same infirmities with regard to non-repudiation as a multiparty key system envisioned by Ford et al.

Ford et al teach away from this invention, and do not suggest it.

The applicant respectfully traverses the assertion of official notice and requests a reference or affidavit of the examiner.

The Rejection of Claims 25, 30, 32, 34, 36 and 37 on the basis of Ford et al (Secure Electronic Commerce).

The examiner states in paragraph 19 of the O.A. dated March 12, 2001 that although Ford et al do not state a signed document in their cited work includes template information or approval of credit card information, official notice could be taken that shopping using credit cards is old and very well known. The examiner further states: "In this case, a user inputs information into a template, such as credit card information. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to allow for online transactions in the system of Ford et al."

With due respect, the claims as redrafted and renumbered as 45, 50, 52, 54, and claims 36 and 37 do not refer to credit card transactions. Redrafted claims 52 and 54 and claim 37 do not even refer to template information at all and so with respect to all of the foregoing claims in this paragraph, the rejection seems misplaced and is confusing at best.

In any event, the credit card information that is referenced in renumbered claim 45 is not the card information inputted by the online user but instead refers to the credit card authorization number of the online credit card paying service, which is a different number and is never inputted by the online user.

The applicant respectfully traverses the assertion of official notice and other information outside of the record and requests a reference or affidavit of the examiner.

The Rejection of Claim 31 on the basis of Ford et al (Secure Electronic Commerce) is overcome.

The examiner in paragraph 20 of the O.A. dated March 12, 2001 rejected claim 31, now renumbered as claim 51. The examiner stated that: "Ford et al. show an originator sending a document that includes template information to a trusted third party who authenticates, signs and returns the document. They do not say that tags or codes are employed. Official notice is taken that it is old and well known to employ tags with digital signatures to simplify their use. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include tags with the signatures of Ford et al to make them more practical."

With due respect, first, the statement of the examiner in this paragraph that Ford et al include template information conflicts with an earlier statement of the examiner in paragraph 19 that Ford et al do *not* include template information. (see supra). The earlier statement of the examiner is correct. Ford et al do not mention anywhere the use of template information with regard to trusted third party signatures. Second, the examiner is also correct that Ford et al do not mention anywhere the use of tags or codes with digital signatures. Third, the applicant requests a reference or affidavit that use of tags with digital signatures is old and well-known. The use of xml tags with digital signatures is very recent and the ongoing work of the W3C, at the time of this writing, is still not complete. The integration of tags with digital signatures based upon client side keys and certificates is very new and complex, with increasing interoperability problems emerging.

One of the novel aspects of this invention over prior art is the use of a single server for signing and verifying signatures without any distribution of client side keys and the consequential obviation of a need for digital certificates to link users to keys. This novel idea is gaining acceptance since the filing release of this invention, precisely for the advantages posed by it. See accompanying declaration of John Messing, dated June 11, 2001.

The applicant respectfully traverses the assertion of official notice with regards to tags and codes and other information outside of the record and requests a reference or affidavit of the examiner.

The Rejection of Claims 33 and 39 on the basis of Ford et al (Secure Electronic Commerce) are overcome.

In paragraph 21, the examiner rejected claim 33, which has been renumbered as new claim 53. Using almost identical language and reasoning, the examiner rejected in paragraph 22 claim 39. Because the rejections are almost identical, employ nearly identical reasoning and language, and deal with the same substance, they have been combined for purposes of amendment and response.

With due respect, first, the statement of the examiner in two referenced paragraphs of the O.A. to the effect that Ford et al include template information conflicts with an earlier statement of the examiner in paragraph 19 that Ford et al do *not* include template information. (see supra). The first statement of the examiner is correct. Ford et al do not mention anywhere the use of template information with regard to trusted third party signatures. Secondly, the examiner is correct in both paragraphs when he states in identical language that Ford et al "do not say that the signature is a MAC or that the encryption key is a product of the document's unique identifier." Ford et al do not include any discussion, hint or suggestion regarding the use of symmetric keys or unique document identifiers, both of which are alien to their thesis regarding the use of asymmetric keys and PKI for signature security.

The examiner does however take official notice that "MACs are old and well-known as using symmetric keys to provide something that works as a signature," and concludes that it would have been obvious "to use keys derived from the document to be signed to sign the documents of Ford et al."

With all due respect, Ford et al teach exactly the opposite from the official notice that is asserted. They expressly state on p. 320 as follows. (See the amended 1449 with attached pages, filed herewith):

“Recall that a MAC is a symmetric cryptographic mechanism – both the originator and recipient of a message share a common key. The originator uses the key to generate the MAC and the recipient uses the same key to verify the MAC. This mechanism can provide authentication and data integrity – the recipient can be confident of who originated the message and that the message was not modified, provided it is known that only the two parties possessed the key. However, a MAC cannot provide non-repudiation of the origin of a message because it is not adequate *to convince a third party* as to who originated the message – since two parties possessed the key, either one could equally well have originated the message.” (Emphasis original)

Under the circumstances, Applicant respectfully requests the examiner to reconsider the invocation of official notice. In this invention, only one party, which is the server, ever possesses the symmetric key, both for signing and verifying a signature. Since only one party (the server) and never two parties possesses the symmetric key, the system does not suffer from the same infirmities with regard to non-repudiation as a multiparty key system envisioned by Ford et al.

Ford et al teach away from this invention, and do not suggest it.

The applicant respectfully traverses the assertion of official notice and requests a reference or affidavit of the examiner.

The Rejection of Claim 37 on the basis of Ford et al (Secure Electronic Commerce) is confusing by virtue of a presumed typographical error in a cross reference but should be overcome in substance.

In paragraph 23 of the O.A. dated March 12, 2001, the examiner rejected claim 37. The examiner wrote: “Ford et al show an originator sending a document that includes template information to a trusted third party who authenticates, signs, and returns the document. They do not say that authentication requires a biometric or secret. Official notice is taken that authentication by biometric or secret is old and well known. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate

the originate or Ford et al. using the common method of either biometric identification or proof of knowledge of a secret.”

The heading of the paragraph states that Claim 37 is rejected ... “as applied to claim 36 above.” A discussion of claim 39, not claim 36 immediately precedes the discussion of claim 37. There is no separate discussion anywhere in the O.A. of claim 36. Therefore, the applicant is unsure of the meaning of the heading of paragraph 23 and has by separate filing herewith noticed a probable typographical error and requested action.

However, as to the substance of the discussion included in paragraph 23, with due respect, first, the statement of the examiner to the effect that Ford et al include template information conflicts with an earlier statement of the examiner in paragraph 19 that Ford et al do *not* include template information. (see supra). The first statement of the examiner is correct. Ford et al do not mention anywhere the use of template information with regard to trusted third party signatures. Secondly, Ford et al expressly limit examples of the permissible methods of authentication to very specific ones based upon Kerberos and PKI, as set forth in endnote 35. These include authentication based on local domain security services on a client-server network with public-key or Kerberos authentication and key establishment. Ford et al. do not include passwords or biometrics as permissible identifiers. To the extent that this invention does, Ford et al. teach away from the invention and do not suggest it.

The applicant respectfully traverses the assertion of official notice and requests a reference or affidavit of the examiner.

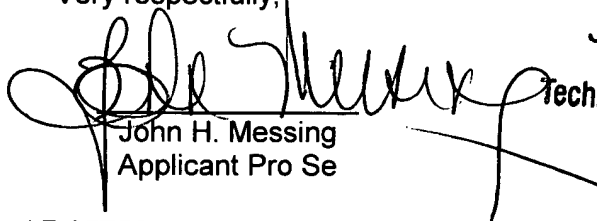
Conclusion

For all of the above reasons, applicant submits that the specification and claims are now in proper form, and that the claims all define patentability over the prior art. Therefore, applicant submits that this application is now in condition for allowance, which action is respectfully solicited.

Conditional Request for Constructive Assistance

Applicant has requested amendment of the specification and claims of this application so that they are proper, definite and define novel structure which is also unobvious. If, for any reason this application is not believed to be in full condition for allowance, applicant respectfully requests the constructive assistance and suggestions of the Examiner pursuant to M.P.E.P. Sections 706.03(d) and 707.07(j) in order that the undersigned can place this application in allowable condition as soon as possible and without the need for further proceedings. Alternatively, if the examiner agrees that patentable subject matter is presented but does not feel that the present claims are technically adequate, applicant respectfully requests the examiner to write acceptable claims pursuant to MPEP 707.07(j).

Very respectfully,


John H. Messing
Applicant Pro Se**RECEIVED**

JUN 19 2001

Technology Center 2100

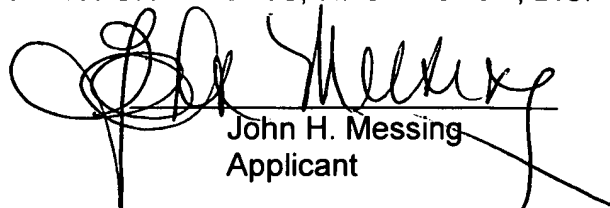
6571 N. Silver Smith Place, Tucson, AZ 85750

Tel.: (520) 547-7933 or (520) 529-3275

Fax: (866) 244-4559

Certificate of mailing: I certify that on the date below this document and referenced documents and attachments will be deposited with the U.S. Postal Service as first class mail in an envelope addressed to: "BOX AF, ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231."

June 12, 2001


John H. Messing
Applicant